John E. Burns
(571) 422-7227- john.edward.burns.jr@gmail.com
https://johnedwardburns.com - https://linkedin.com/johneburnsjr/ - https://github.com/johneburnsjr
Crozet VA

CAREER SUMMARY

System Administrator with 10+ years of IT experience and 7+ years securing identity and access infrastructure across hybrid environments. Skilled in managing Azure AD (Entra ID), Okta, Microsoft Defender, and Office 365 security controls. Proven track record of automating patching, threat response, and identity workflows using PowerShell. Led initiatives in MFA enforcement, vulnerability remediation, and endpoint protection using tools like Nessus, Carbon Black, and Microsoft Sentinel. Currently transitioning into a full-time Cloud Security Engineer role, with hands-on cloud security labs, application security, and an expanding portfolio of security automation and detection projects.

EXPERIENCE

Focused Ultrasound Foundation Charlottesville, VA
System Administrator Aug 2017 - Present

- **Threat Detection & SIEM:** Tuned Splunk dashboards and detection rules for real-time log triage and enhanced threat visibility.
- **Endpoint Protection:** Hardened systems using Carbon Black and Microsoft Defender for Endpoint, automating quarantines and remediation.
- **Incident Response:** Investigated security events using Defender, NinjaOne, and Windows logs; supported internal threat resolution.
- **Security Automation:** Built PowerShell scripts for patching, access control, and incident reporting to streamline operations.
- **Identity & Access Management:** Enforced MFA, conditional access, and RBAC policies via Azure AD and Okta across 60+ hybrid-joined devices.
- **Security Awareness Training:** Delivered phishing simulations and training to 50+ staff, reducing click rates by 30%.

Innovative Refrigeration Systems Lyndhurst, VA
IT Support Specialist Jan 2016 – July 2017

- **IT Asset Management**: Inventoried, deployed, and troubleshot company-wide **computer assets and network devices**.
- **Access Control & Permissions**: Managed **Active Directory user permissions & shared drives**.
- **Documentation & SOPs**: Created technical documentation and SOPs for **IT staff and web development teams**.

District of Columbia Army National Guard (Deployed in Kuwait)
Information Management Officer Aug 2014 – July 2015

- **Active Directory Management**: Ensured **user access security compliance** on military networks.
- **System Administration**: Installed and maintained **25 Windows-based computers** in an unclassified network.
- **Security Monitoring**: Maintained and monitored **66 CCTV cameras & 4 DVR systems**, saving **$2,000** of Army property.

National Guard HQ Washington, D.C.
Joint Operations Center Operator Jan 2013 – Aug 2014

- **Network & User Administration**: Managed **Active Directory passwords & user access**.
- **Incident Handling & Crisis Communication**: Coordinated emergency procedures & FEMA communication drills.

CERTIFICATIONS

(ISC)2 SSCP: ID: 682974
CompTIA CYSA+: WZWKGP6NSK411RSL
CompTIA Security+: R6MMJRTM1GV4Q7KN
CompTIA Network+: 59586GHMC31QK6BB

EDUCATION

- **George Mason University** | Certificate in **Information Technology, Security** (2011 – 2013)
- **Johnson & Wales University** | **B.S. Food Service Management** (2001 – 2005)

TECHNICAL SKILLS AND TOOLS

Identity & Access Management (IAM)

- Active Directory (AD) – User provisioning, group policy and role-based access control (RBAC).
- Microsoft Entra ID (Azure AD) – Cloud-based identity management and Devices.
- Office 365 Security & Compliance – Set up and manage Intune and SharePoint permissions.
- Okta – Identity federation, MFA enforcement, and SSO integration.
- NinjaOne – Endpoint management and security monitoring.

Cybersecurity & Threat Detection

- Microsoft Defender for Endpoint – Endpoint protection, security hardening, and threat response.
- Cloud Security: Microsoft Entra ID (Azure AD), Microsoft Defender for Cloud, Intune, Conditional Access
- Splunk – Security Information and Event Management (SIEM), log analysis, and incident response.
- Nessus – Vulnerability scanning, risk assessments, and security patch compliance.
- Firewalls & Network Security – WatchGuard, Windows Firewall, rule and VPN configuration.
- Security Awareness Training – Employee phishing simulations and policy enforcement.

ADDITIONAL

- **OSINT & Threat Intelligence**: Conducted **Open-Source Intelligence (OSINT) investigations** for **CTF competitions** (e.g., **RVAsec CTF**) and **real-world cybersecurity tasks**, enhancing analytical and investigative skills.
- **Hands-On Cybersecurity Training**: Actively participate in **TryHackMe challenges**, focusing on **penetration testing, forensics, and security operations** to strengthen practical skills.
- **Industry Research & Continuous Education**: Stay updated on **emerging cybersecurity threats, tools, and best practices** by following industry-leading sources, including the **SecurityNow podcast, cybersecurity blogs, and security conferences**.